02-28-00

A

Please type a plus sign (+) inside this box

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

This form is a Replica of PTO/SB/05 (12/97)
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

02/25/00 U.S. PTO

UTILITY PATENT APPLICATION TRANSMITTAL

(only for new nonprovisionals under 37 CFR 1.53(b))

Attorney Docket No.	H16-26156	Total Pages	
First Named Inventor or Application Identifier			
JIANDONG HUANG, ET AL.			
Express Mail Label No. **EM512495449US**			

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, DC 20231

JC564 U.S. PTO
09/513010
02/25/00

1. [X] Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. [X] Specification
(preferred arrangement set forth below)
- Descriptive title of the invention
- Cross Reference to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) (35 USC 113)[Total Sheets 3]

4. Oath or Declaration [Total Pages]
a. [ ] Newly executed (original or copy)
b. [ ] Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 Below]
i. [ ] DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. [ ] Incorporation By Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath of declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. [ ] Microfiche Computer Program (Appendix)

7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. [ ] Computer Readable Copy
b. [ ] Paper Copy (identical to computer copy)
c. [ ] Statement verifying identity of above copies.

ACCOMPANYING APPLICATION PARTS

8. [ ] Assignment Papers (cover sheet & document(s))
9. [ ] 37 CFR 3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
10. [ ] English Translation Document (if applicable)
11. [ ] Information Disclosure Statement (ISD)/PTO-1449 [ ] Copies of IDS Citations
12. [ ] Preliminary Amendment
13. [X] Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. [ ] Small Entity Statement(s) [ ] Statement filed in prior application, Status still proper and desired
15. [ ] Certified Copy of Priority Document(s)
(if foreign priority claimed)
16. [X] Other: Unexecuted Oath

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:
[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: _____

18. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label **000128** (Insert Customer No. or Attach bar code label here) or [ ] Correspondence Address Below

NAME	IAN D. MACKINNON				
	PATENT SERVICES DEPARTMENT				
ADDRESS	HONEYWELL INTERNATIONAL INC.				
	101 COLUMBIA ROAD				
CITY	MORRISTOWN	STATE	NEW JERSEY	ZIP CODE	07962
COUNTRY	USA	TELEPHONE	612/951-0612	FAX	612/951-0649

Burden Hour Statement: This [illegible] ed to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any to complete this from should be sent to the Chief Information Officer, Patent and Trademark Office, ES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents Box

Express Mail: EM512495449US
February 25, 2000
Ian D. MacKinnon, Atty.
Jiandong Huang, et al, Inventors
MULTIPLE NETWORK FAULT TOLERANCE VIA REDUNDANT NETWORK CONTROL

Multiple Network Fault Tolerance via Redundant Network Control

Field of the Invention

The invention relates generally to computer networks, and more specifically to a method and apparatus providing a fault-tolerant network having a redundant connection to network nodes able to detect and recover from multiple network faults.

Notice of Copending Applications

This application is related to the following copending applications, which are hereby incorporated by reference:

"Fault Tolerant Networking", serial number 09/188,976; and

Atty. docket number 256.045us1

Background of the Invention

Computer networks have become increasingly important to communication and productivity in environments where computers are utilized for work. Electronic mail has in many situations replaced paper mail and faxes as a means of distribution of information, and the availability of vast amounts of information on the Internet has become an invaluable resource both for many work-related and personal tasks. The ability to exchange data over computer networks also enables sharing of computer

Express Mail: EM512495449US
February 25, 2000
Ian D. MacKinnon, Atty.
Jiandong Huang, et al, Inventors
MULTIPLE NETWORK FAULT TOLERANCE VIA
REDUNDANT NETWORK CONTROL

resources such as printers in a work environment, and enables centralized network-based management of the networked computers.

For example, an office worker's personal computer may run software that is installed and updated automatically via a network, and that generates data that is printed to a networked printer shared by people in several different offices. The network may be used to inventory the software and hardware installed in each personal computer, greatly simplifying the task of inventory management. Also, the software and hardware configuration of each computer may be managed via the network, making the task of user support easier in a networked environment.

Networked computers also typically are connected to one or more network servers that provide data and resources to the networked computers. For example, a server may store a number of software applications that can be executed by the networked computers, or may store a database of data that can be accessed and utilized by the networked computers. The network servers typically also manage access to certain networked devices such as printers, which can be utilized by any of the networked computers. Also, a server may facilitate exchange of data such as e-mail or other similar services between the networked computers.

Connection from the local network to a larger network such as the Internet can provide greater ability to exchange data, such as by providing Internet e-mail access or access to the World Wide Web. These data connections make conducting business via the Internet practical, and have contributed to the growth in development and use of computer networks. Internet servers that provide data and serve functions such as e-

commerce, streaming audio or video, e-mail, or provide other content rely on the operation of local networks as well as the Internet to provide a path between such data servers and client computer systems.

But like other electronic systems, networks are subject to failures. Misconfiguration, broken wires, failed electronic components, and a number of other factors can cause a computer network connection to fail, leading to possible inoperability of the computer network. Such failures can be minimized in critical networking environments such as process control, medical, or other critical applications by utilization of backup or redundant network components. One example is use of a second network connection linking critical network nodes providing the same function as the first network connection. But, management of the network connections to facilitate operation in the event of a network failure can be a difficult task, and is itself subject to the ability of a network system or user to properly detect and compensate for the network fault. Furthermore, when both a primary and redundant network develop faults, exclusive use of either network will not provide full network operability. What is needed is a method and apparatus to detect and manage the state of a network of computers utilizing redundant communication channels.

Summary of the Invention

The present invention provides a method and apparatus for detecting and managing the state of a computer network comprising network nodes with redundant network connections, and for recovering from multiple network faults. In one

embodiment, a network status table is employed in each node to manage data related to the network state between the node and other nodes in the network. In various embodiments, rerouting of data is managed independently such that a communication path is independently selected for sending data from a node to a connected node and for receiving data from the connected node. The invention in some embodiments is operable to route data through one or more intermediate nodes where direct connection between a pair of nodes is not possible.

Brief Description of the Figures

Figure 1 shows a diagram of a computer network with multiple nodes having primary and redundant network connections, consistent with an embodiment of the present invention.

Figure 2 shows an example of a network status table, consistent with an embodiment of the present invention.

Figure 3 shows a flowchart of a method of managing the state of a network of nodes having primary and redundant network connections, consistent with an embodiment of the present invention.

Detailed Description

In the following detailed description of sample embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific sample embodiments in which the

invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, and other changes may be made without departing from the spirit or scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the invention is defined only by the appended claims.

The present invention provides a method and an apparatus for detecting and managing the state of network connections to facilitate operation of a redundant network in the event of a network failure. The invention is capable of compensating for multiple network faults, including faults in both the primary and the redundant network. In some embodiments, the invention selects either the primary or the redundant network connection for communicating data between each pair of network nodes, such that the network may continue to be fully operational so long as at least one connection is operable to transmit data and one connection is operable to receive data between each pair of network nodes.

The invention in various forms is implemented using an existing network technology, such as Ethernet. In one such embodiment, two connections between each node are made via Ethernet connections — a primary network connection and a redundant network connection. In some such embodiments, off-the-shelf network adapters are utilized, and the invention controls the operation of the network adapters and manages communication via software executing on the computerized nodes. It is not critical for purposes of the invention which connection is the primary connection

and which is the redundant connection, as the connections are physically and functionally similar. In the example embodiment discussed here, the primary and redundant network connections are interchangeable and are assigned names primarily for the purpose of distinguishing the networks from each other.

Figure 1 illustrates an exemplary network with four nodes 101, 102, 103 and 104. A primary network 105 and a redundant network 106 links each node to the other nodes of the network, as indicated by the directional lines connecting the nodes to each of the networks. To understand how the invention is operable to compensate for multiple network failures, the connection from node 3 at 103 to primary network 105 is broken such that node 3 cannot transmit data to network 105 as shown at 107. Also, the connections linking node 4 at 104 to the redundant bus 106 are broken such that node 4 cannot receive data from the redundant bus as shown at 108 and cannot transmit data to the redundant bus as shown at 109.

In a typical redundant network system, failure of a single connection between the primary network and a node such as is shown at 107 would cause all nodes on the network to switch to communicating via the redundant bus 106. In the network configuration shown in Figure 1, connections between node 4 and the redundant bus are also inoperable, making operation of the network using the redundant bus impossible. Such multiple failures make the network inoperable when exclusively using either the primary or redundant bus.

The present invention provides a solution to this problem and enables communication between all network nodes during multiple failures such as are shown

in Figure 1 by use of network status data and intelligent routing of data. In some embodiments of the invention, the network status data is stored in a network status table as shown in Figure 2.

Figure 2 illustrates an example of a network status table for node 3 of the network of Figure 1, and contains data indicating the ability of node 3 to receive data from other nodes and the ability of other nodes to receive data from node 3. Specifically, the "Received Data OK" columns indicate the ability of node 3 to receive data from each of nodes 1, 2 and 4 on both the primary and redundant networks. The table indicates with an "X" that node 3 cannot receive data from node 4 over the redundant network connection, and indicates that node 3 can receive data from all other nodes via both the primary and redundant network connections with an "OK". The "X" indicating node 3's inability to receive data from node 4 is the result of the broken data transmit connection 109 between the redundant network 106 and node 4 (104).

The "Other Node Report Data" columns represent the data reported to node 3 by other nodes regarding the ability of the various other nodes to receive data from node 3. Because node 3's connection to the primary network 105 is broken at 107 such that node 3 cannot send data over the connection, nodes 1, 2 and 4 are unable to receive data from node 3 on the primary network and so an "X" indicates a node 3 failure for each of these nodes. Also, the data connection between node 4 and the redundant network is broken at 108 such that node 4 cannot receive data from the redundant network, so an "X" also indicates that node 4 is unable to receive data from

node 3 in the node "4" column of the "Node 3 Redundant" row.

The determination of whether a node can receive data from another node is made in various embodiments using special-purpose diagnostic data signals, using network protocol signals, or using any other suitable type of data sent between nodes. The data each node provides to other nodes to populate the "Other Node Report Data" must necessarily be data which includes the data to be communicated between nodes, and is in one embodiment a special-purpose diagnostic data signal comprising the node data to be reported.

From the data in the network status table of Figure 2, the state of the various network connections can be determined and a suitable connection for communication between each pair of network nodes can be selected. In the example of Figures 1 and 2, nodes 1 and 2 are fully operational and may use either connection to communicate, and nodes 3 and 4 each have a fully operational connection to either the primary or redundant networks. Therefore, only nodes 3 and 4 are unable to communicate over either the primary or redundant network exclusively. Node 3 cannot send data to the primary network, and node 4 cannot send or receive data from the redundant network, but node 3 can receive data from node 4 via the primary network. In some embodiments of the invention, node 3 cannot send data to node 4 because no operable direct path over either the primary or redundant networks exists to send data.

In other embodiments of the invention, node 3 may transmit the data to node 4 via another node with an "OK" indication for either network in the "Other Node Report Data" rows of the table such as node 1 or node 2. In such embodiments, the

"OK" nodes or intermediate nodes are known to be able to receive data from node 3, and can retransmit the data to node 4 via their fully functional primary network connections. This allows communication between two nodes where multiple network failures prevent direct communication between two nodes. In further embodiments, the intermediate node to which the data is routed is selected via polling the intermediate nodes to select a node that indicates it is able to retransmit data to node 4 by evaluation of the data in each of the intermediate nodes' network status table. In various embodiments of the invention, the intermediate nodes may comprise networked computers as in the example above, may comprise a direct connection between networks, may comprise a router or bridge, may comprise a special-purpose intermediate node hardware device, or may be implemented in any other way that provides the ability to suitably communicate signals between the two networks.

Figure 3 is a flowchart illustrating a method of practicing one embodiment of the present invention. At 301, each node determines the state of the primary network connection linking it to each other node. Also, the state of the redundant network connection linking each node to each other node is determined at 302. The state of the primary and redundant connections between each pair of nodes can is determined in various embodiments by searching the connections for existing data such as valid data or protocol packets, or by use of special-purpose diagnostic messages. This network connection state data is used at 303 to build the "Received Data OK" portion of a network status table for each node, and the nodes exchange data with each other at 304 to complete the "Other Node Report Data" portion of the network status table. The

network status table is updated regularly, and is monitored at 305 to determine whether a network connection has failed and requires rerouting of data.

At 306, the node determines by examination of the network status table whether a direct connection for transmitting and receiving data between the pair of nodes with a failed connection can be made. If a connection can be made, such as by transmitting data via the primary network connection and receiving data through the redundant network connection, the data is rerouted trough the direct connections at 307 and monitoring for additional failures resumes at 305. If a direct connection cannot be made, data is rerouted through one or more intermediate nodes at 308 to facilitate communication, as was described in accordance with the multiple network failure example illustrated in Figures 1 and 2. Again, once a data path through one or more intermediate nodes has been selected monitoring for additional network failures resumes at 305.

The present invention provides a method and apparatus that enable a network with primary and redundant network connections to manage routing of data through the network such that multiple network failures can be compensated for. In some embodiments, the invention includes rerouting data that cannot be transferred directly between two nodes to intermediate nodes which are able to facilitate communication between the nodes. The invention also incorporates construction and use of a network status table in some embodiments for managing data related to the network state. The invention includes in various embodiments a method for managing the state of the network, software for execution on a computer for managing the state of the network,

and a hardware network interface that is operable to manage the state of the network.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the invention. It is intended that this invention be limited only by the claims, and the full scope of equivalents thereof.

Claims

1. A method of managing the state of a computer network with redundant network connections, comprising:

determining the state of a primary network connection between each pair of networked nodes;

determining the state of a redundant network connection between each pair of networked nodes; and

selecting either the primary network connection or the redundant network connection for sending and receiving data between each pair of networked nodes, such that the network path selected to be used to communicate is selected independently based on the determined network states for each pair of networked nodes.

2. The method of claim 1, further comprising building a network status table that indicates results of determining the state of primary and redundant network connections between each pair of networked nodes.

3. The method of claim 2, wherein the network status table comprises data representing network status based on data received at a node from other network nodes.

Express Mail: EM512495449US
February 25, 2000
Ian D. MacKinnon, Atty.
Jiandong Huang, et al, Inventors
MULTIPLE NETWORK FAULT TOLERANCE VIA
REDUNDANT NETWORK CONTROL

4. The method of claim 3, wherein the data received at a node from other networked nodes comprises a diagnostic message.

5. The method of claim 4, wherein the data received at a node from other networked nodes comprises data representing the ability of the other nodes to receive data from other different network nodes.

6. The method of claim 2, wherein the network status table comprises data representing network status based on a node's ability to send data to other nodes.

7. The method of claim 3, wherein the network status table further comprises data representing network status based on a node's ability to send data to other nodes.

8. The method of claim 1, wherein selecting the primary or redundant network connection for communication between each pair of networked nodes comprises:

selecting the primary network connection if the state of the primary network connection is determined to be operable; and

selecting the redundant network connection if the state of the primary network connection is determined to be inoperable.

9. The method of claim 1, wherein selecting the primary or redundant network connection for communication between each pair of networked nodes comprises:

selecting the primary network connection to transmit data if the state of the primary network connection is determined to be operable to transmit data;

selecting the primary network connection to receive data if the state of the primary network connection is determined to be operable to receive data;

selecting the redundant network connection to transmit data if the state of the primary network connection is determined to be inoperable to transmit data; and

selecting the redundant network connection to receive data if the state of the primary network connection is determined to be inoperable to receive data.

10. The method of claim 1, wherein selecting a connection for sending and receiving data between each pair of network nodes comprises selecting a connection for sending and receiving data from a first node to one or more connected intermediate nodes, and selecting a connection for sending and receiving data from an intermediate node to a second node.

11. A computer network interface, the interface operable to:

determine the state of a primary network connection between the network interface and the network interfaces of other network nodes;

determine the state of a redundant network connection between the network interface and the network interfaces of other network nodes; and

select either the primary network connection or the redundant network connection for communication with each of the other network nodes, such that the

network connection selected is selected independently based on the determined network states for each other network node.

12. The computer network interface of claim 11, the interface further comprising a network status table that indicates results of the determination of the state of the primary and redundant network connections between the computer network interface and the network interfaces of other network nodes.

13. The computer network interface of claim 12, wherein the network status table comprises data representing network status based on data received at a node from other network nodes.

14. The computer network interface of claim 13, wherein the data received at a node from other networked nodes comprises a diagnostic message.

15. The computer network interface of claim 14, wherein the data received at a node from other networked nodes further comprises data representing the ability of the other nodes to receive data from other different network nodes.

16. The computer network interface of claim 12, wherein the network status table comprises data representing network status based on a node's ability to send data to other nodes.

17. The computer network interface of claim 13, wherein the network status table further comprises data representing network status based on a node's ability to send data to other nodes.

18. The computer network interface of claim 11, wherein selecting either the primary network connection or the redundant network connection for communication with each of the other network nodes comprises:

selecting the primary network connection if the state of the primary network connection is determined to be operable; and

selecting the redundant network connection if the state of the primary network connection is determined to be inoperable.

19. The computer network interface of claim 11, wherein selecting either the primary network connection or the redundant network connection for communication with each of the other network nodes comprises:

selecting the primary network connection to transmit data if the state of the primary network connection is determined to be operable to transmit data;

selecting the primary network connection to receive data if the state of the primary network connection is determined to be operable to receive data;

selecting the redundant network connection to transmit data if the state of the primary network connection is determined to be inoperable to transmit data; and

selecting the redundant network connection to receive data if the state of the primary network connection is determined to be inoperable to receive data.

20. The computer network interface of claim 11, wherein selecting a connection for sending and receiving data between each pair of network nodes comprises selecting a connection for sending and receiving data from a first node to one or more connected intermediate nodes, and selecting a connection for sending and receiving data from an intermediate node to a second node.

21. A machine-readable medium with instructions thereon, the instructions when executed on a computer operable to cause the computer to:

determine the state of a primary network connection between the network interface and the network interfaces of other network nodes;

determine the state of a redundant network connection between the network interface and the network interfaces of other network nodes; and

select either the primary network connection or the redundant network connection for communication with each of the other network nodes, such that the network connection selected is selected independently based on the determined network states for each other network node.

22. The machine-readable medium of claim 21, the instructions further operable to cause a computer to create and maintain a network status table that indicates results of

the determination of the state of the primary and redundant network connections between the computer network interface and the network interfaces of other network nodes.

23. The machine-readable medium of claim 22, wherein the created network status table comprises data representing network status based on data received at a node from other network nodes.

24. The machine-readable medium of claim 23, wherein the data received at a node from other networked nodes comprises a diagnostic message.

25. The machine-readable medium of claim 24, wherein the data received at a node from other networked nodes further comprises data representing the ability of the other nodes to receive data from other different network nodes.

26. The machine-readable medium of claim 22, wherein the created network status table comprises data representing network status based on a node's ability to send data to other nodes.

27. The machine-readable medium of claim 23, wherein the network status table further comprises data representing network status based on a node's ability to send data to other nodes.

28. The machine-readable medium of claim 21, wherein selecting either the primary network connection or the redundant network connection for communication with each of the other network nodes comprises:

selecting the primary network connection if the state of the primary network connection is determined to be operable; and

selecting the redundant network connection if the state of the primary network connection is determined to be inoperable.

29. The machine-readable medium of claim 21, wherein selecting either the primary network connection or the redundant network connection for communication with each of the other network nodes comprises:

selecting the primary network connection to transmit data if the state of the primary network connection is determined to be operable to transmit data;

selecting the primary network connection to receive data if the state of the primary network connection is determined to be operable to receive data;

selecting the redundant network connection to transmit data if the state of the primary network connection is determined to be inoperable to transmit data; and

selecting the redundant network connection to receive data if the state of the primary network connection is determined to be inoperable to receive data.

30. The machine-readable medium of claim 21, wherein selecting a connection for

sending and receiving data between each pair of network nodes comprises selecting a connection for sending and receiving data from a first node to one or more connected intermediate nodes, and selecting a connection for sending and receiving data from an intermediate node to a second node.

Document ID: 0000000000

Abstract

The present invention provides a method and apparatus for detecting and managing the state of a computer network comprising network nodes with redundant network connections, and for recovering from multiple network faults. In one embodiment, a network status table is employed in each node to manage data related to the network state between the node and other nodes in the network. In various embodiments, rerouting of data is managed independently such that a communication path is independently selected for sending data from a node to a connected node and for receiving data from the connected node. The invention in some embodiments is operable to route data through one or more intermediate nodes where direct connection between a pair of nodes is not possible.

Express Mail: EM512495449US
February 25, 2000
Ian D. MacKinnon, Atty.
Jiandong Huang, et al, Inventors
MULTIPLE NETWORK FAULT TOLERANCE VIA
REDUNDANT NETWORK CONTROL

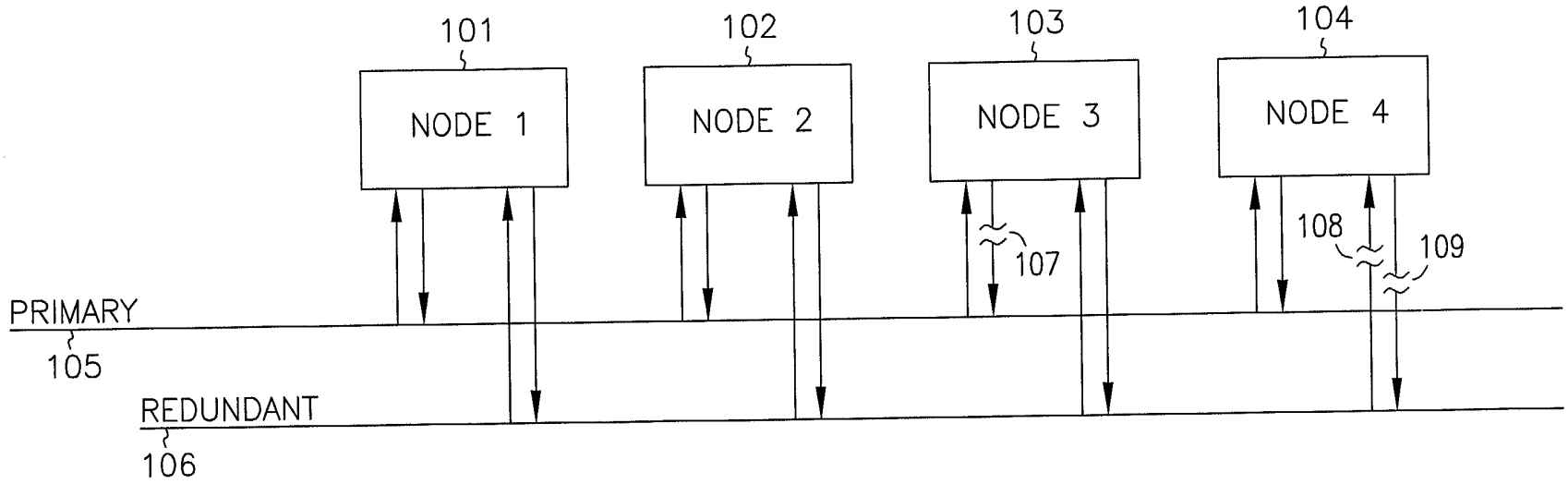

Fig.1

NODE 3 NETWORK STATUS TABLE

RECEIVED DATA OK			OTHER NODE REPORT DATA	
NODE#	PRIMARY	REDUNDANT	NODE 3 PRIMARY	NODE 3 REDUNDANT
1	OK	OK	X	OK
2	OK	OK	X	OK
–	–	–	–	–
4	OK	X	X	X

Fig.2

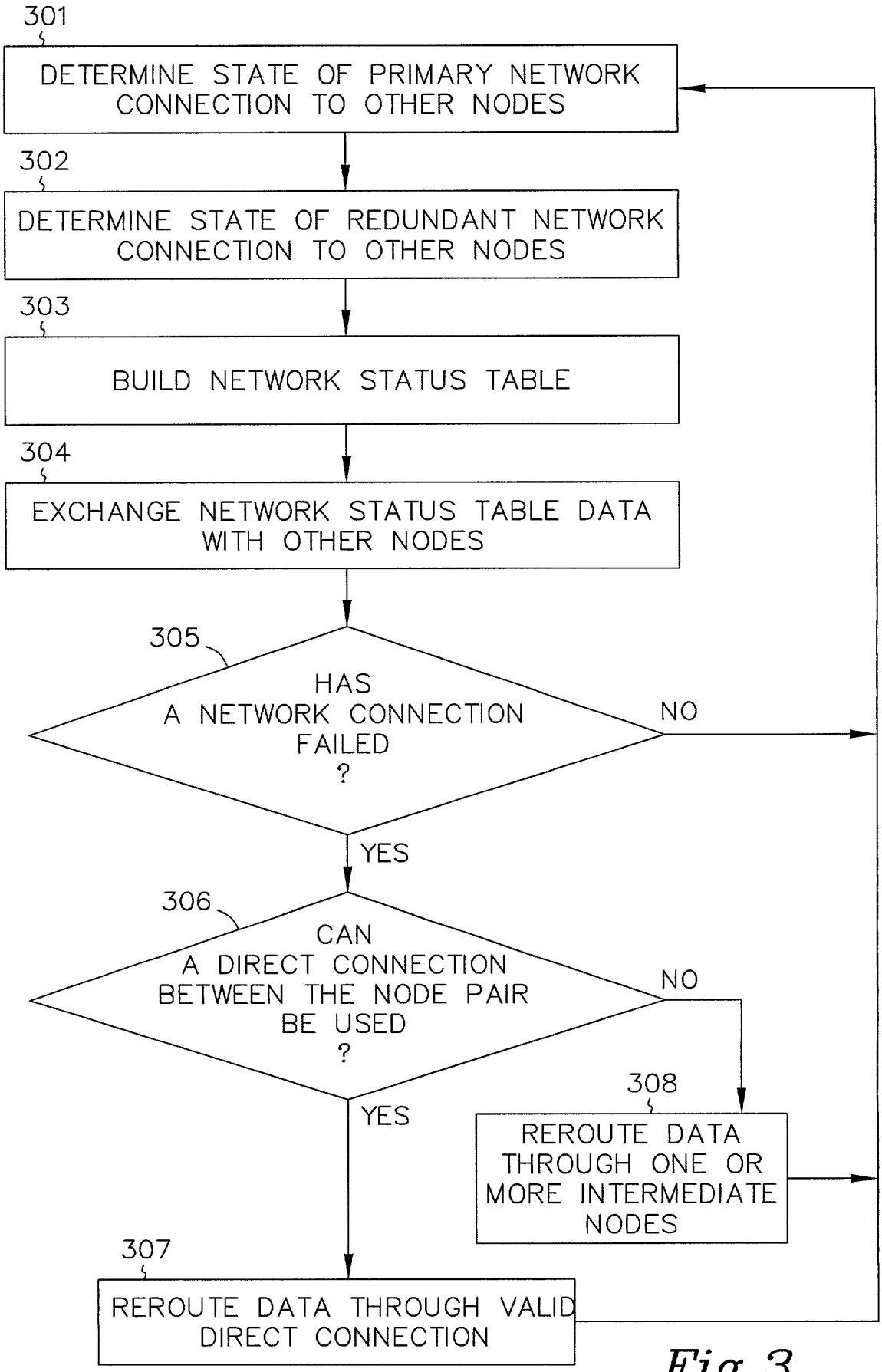
301
DETERMINE STATE OF PRIMARY NETWORK CONNECTION TO OTHER NODES
302
DETERMINE STATE OF REDUNDANT NETWORK CONNECTION TO OTHER NODES
303
BUILD NETWORK STATUS TABLE
304
EXCHANGE NETWORK STATUS TABLE DATA WITH OTHER NODES
305
HAS A NETWORK CONNECTION FAILED ?
NO
YES
306
CAN A DIRECT CONNECTION BETWEEN THE NODE PAIR BE USED ?
NO
YES
308
REROUTE DATA THROUGH ONE OR MORE INTERMEDIATE NODES
307
REROUTE DATA THROUGH VALID DIRECT CONNECTION

Fig.3

Application for United States

PATENT
H16-26156
Customer Number: 000128

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

MULTIPLE NETWORK FAULT TOLERANCE VIA REDUNDANT NETWORK CONTROL

The specification of which

(check one) _X_ is attached hereto
_____ was filed on _____ as
Application Serial No._____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).*

I hereby claim foreign priority benefits under Title 35, United States Code §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			**PriorityClaimed**	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: JOHN G. SHUDY, JR. (Reg. No. 31,214) and IAN D. MACKINNON (Reg. No. 34,660). Address all telephone calls to IAN D. MACKINNON at telephone number (612) 951-0612.

Address all correspondence to IAN D. MACKINNON, Honeywell Inc., Honeywell Plaza, P.O. Box 524, Office of General Counsel, MN12-8251, Minneapolis, Minnesota 55440-0524.

Express Mail: EM512495449US
February 25, 2000
Ian D. MacKinnon, Atty.
Jiandong Huang, et al, Inventors
MULTIPLE NETWORK FAULT TOLERANCE VIA
REDUNDANT NETWORK CONTROL

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor **JIANDONG HUANG**

Inventor's Signature _____ Date _____, 19___

Residence Plymouth, Minnesota (Hennepin County)

Citizenship USA

Post Office Address 4365 Juneau Lane

Plymouth, Minnesota 55446

Full Name of Second Joint Inventor, If Any **SEJUN SONG**

Inventor's Signature _____ Date _____, 19___

Residence Minneapolis, Minnesota (Hennepin County)

Citizenship Republic of Korea

Post Office Address 1026 27th Avenue S.E. Apt. F

Minneapolis, Minnesota 55414

Full Name of Third Joint Inventor, If Any **TONY J. KOZLIK**

Inventor's Signature _____ Date _____, 19___

Residence Phoenix, Arizona (Maricopa County)

Citizenship USA

Post Office Address 2936 W. Morrow Drive

Phoenix, Arizona 85027

Full Name of Fourth Joint Inventor, If Any **RONALD J. FREIMARK**

Inventor's Signature _____ Date _____, 19___

Residence Scottsdale, Arizona (Maricopa County)

Citizenship USA

Post Office Address 13014 N. 62nd Street

Scottsdale, Arizona 85254

Full Name of Fifth Joint Inventor, If Any **JAY W. GUSTIN**

Inventor's Signature _____ Date _____, 19___

Residence Scottsdale, Arizona (Maricopa County)

Citizenship USA

Post Office Address 6226 E. Joan De Arc Avenue

Scottsdale, Arizona 85254

*Title 37, Code of Federal Regulations §1.56:

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.